20268

NOTICE OF DATA BREACH

We are sending this letter to inform you of a data breach involving our tax software company. This letter will be followed up with an additional letter if more information is made available to us, but given the sensitive nature of the information potentially exposed, we wanted to notify you of the matter as soon as possible.

What Happened?
As of April 23, 2021:
On April 22, 2021, our software company notified our firm of a data security incident involving multiple firms nationally and client 2020 tax returns being filed fraudulently. After initial investigation, we have discovered that the perpetrator(s) filed these returns from a location outside of our office and network, and between March 30, 2021 and April 7, 2021, fraudulently filed tax returns. We have identified and are in the process of resolving the fraudulently filed tax returns with the IRS and tax software company. Although we are unaware of any false tax returns having been filed under your name or company, we are notifying you of this incident because your information may have been exposed.

What Information Was Involved?
If you are an individual, this information may have included your name, gender, date of birth, telephone number(s), address, social security number, all employment (W-2) information, 1099 information, as well as direct deposit bank account information, including account number and routing information (if provided to us). Further, supporting documentation including brokerage statements and other types of specific documents you may also have provided to us.

If you are an entity, this information may have included your company name, Federal Employer Identification Number, address, telephone number; employee and/or 1099-recipient information; partner, shareholder/officer or beneficiary names, addresses, social security numbers; and/or other information stored in our computer network files.

The protection and privacy of your information has always been a top priority for our firm. We have no words to express how devastating it is to have had this happen.

What We Have Done So Far:
Based on the **diligent investigative work** of **both** our IT consultant and investigation team at the tax software company:

- No malware has been found on our computers.
- No breaches of network firewalls, computers and security protections has been found on our network.
- All network firewalls, computers and security protections are confirmed to be properly functioning.

We are working with **appropriate agencies** on your behalf regarding the following:

- The **IRS** has been made aware of all the fraudulent filings. We are working with the IRS and tax software company to assist in their investigation and interruption of intent of the cyber intruder(s).
- We are awaiting further counsel recommendations.

- While we are confident the security breach did not occur within our office or network, we are being overly cautious and being as proactive as possible to protect our clients from any potential harm.

What You Can Do:

- Given the breadth of information potentially exposed, we strongly recommend you are vigilant in reviewing all bank account and brokerage statements, as well as free credit reports.
- We suggest that have a conversation with your bank regarding the monitoring to be provided by them as well as yourselves. It is also recommended that you change your **passwords** on all accounts, bank and brokerage.
- Please go to www.identitytheft.gov , click "Get Started", click "Someone filed a Federal tax return – or claimed an economic stimulus payment – using my information" (even though they have not as of the date of the notice, click this), continue through the prompts. At the end of process, the IRS Form 14039 Identity Theft Affidavit will be generated and filed electronically with the IRS. This is an additional layer of protection that is available to you.
- You can call the three major credit agencies and place a 90-day fraud alert on your accounts. If you want to pursue that further, their contact information is:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
https://www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

- You are also entitled to a free credit report every year from each of these three agencies at: https://www.annualcreditreport.com
- If you suspect identity theft, report it to law enforcement, including the FTC at: https://www.identitytheft.gov/Assistant#

Again, the protection and privacy of your information has always been a top priority for our firm. Please be reassured that we have acted promptly and swiftly to protect your private information and should any issues arise with the IRS, the IRS has assured us you will not be held liable for the actions of this perpetrator (s).

Sincerely,

Cozby & Company LLC

Notice of Reported Fraudulent Tax Return Filing

We are sending this letter to inform you of a data breach involving our tax software company. This letter is notification that your personal information has been compromised. This letter will be followed-up with an additional letter, but **we wanted to provide information and some further Next Steps to help you protect yourself.**

What Happened?
As of April 23, 2021:

- On April 22, 2021, our software company notified our firm of a data security incident involving multiple firms nationally and client 2020 tax returns being filed fraudulently.
- After initial investigation, we have discovered that the perpetrator(s) filed these returns from a location outside of our office and network, and between March 30, 2021 and April 7, 2021, fraudulently filed tax returns.
- Our tax software company reported to us that the IRS reported to them that your tax return had been e-filed.
- Knowing that we had not filed the return, and after speaking with the software company and the IRS, it became evident that someone, other than you or us, had fraudulently filed your return.

What We Have Done So Far: After additional, thorough investigation of our IT Company and Investigative Team at Software Company:

- No malware has been found on our computers.
- No breaches of network firewalls, computers and security protections has been found on our network.
- All network firewalls, computers and security protections are confirmed to be properly functioning.
- The perpetrator appears to have been **targeting returns not filed from multiple firms,** seeking to **change returns to provide large amounts of refunds, sent by direct deposit to a new bank account in the cyber intruder's bank routing and account number.**

What Information Was Involved?

- A false and fraudulently filed tax return had been filed using your name and social security number, and that the perpetrator would also have been able to see any direct deposit banking information you may have provided to us.
- The information exposed may have included: your name, gender, date of birth, telephone number(s), address, social security number(s), EIN number(s); all employment (W-2) information, 1099 information, as well as correspondence and/or brokerage statements and other documents you provided to us to complete your tax return.

We are working with appropriate agencies on your behalf regarding the following:

- The IRS has been made aware of all the fraudulent filings. We are working with the IRS and tax software company to assist in their investigation and interruption of intent of the cyber intruder(s).
- We will be filing Identity Theft Affidavits electronically through the IRS website in the coming days on your behalf.
- We are awaiting further counsel recommendations.
- While we have no evidence the security breach occurred within our network, we are being overly cautious and being as proactive as possible to protect our clients from any potential harm.

Fraudulent Tax Filings Info:

- Importantly, **the IRS, is working to have placed your account on Fraud Alert**. We have also provided the IRS with the routing number and bank account number opened, by the perpetrator who was seeking the refund to be accessible to himself.
- **We are working to stop these payments.** However, if the "bad guy" was successful in getting a refund based on this fraudulent filing of your return, **the IRS has assured us that you will not be penalized monetarily for the fraudulent refund.**
- **In some cases, the refund had already been released by the IRS**, and a refund of a paper check will be mailed to you. **Do *not* cash that check. VOID it, and then get the check to us. We will forward it to the IRS for credit to your account.**

- **Please send a copy to our office of any IRS letter that you receive, as soon as possible upon receipt.** We can contact the IRS. We are obtaining clarification from the IRS on how to respond to its variety of computer-generated form letters, depending on where your return was in its processing when we filed the Fraud Alert: or If your false return had already been completely processed.

The IRS has indicated in a non-pandemic year that the expected time to resolve fraudulent filings is 6 months. With the pandemic, they have advised it can easily take over a year. There is nothing that can be done to speed this process up for you.

Moving forward, once resolved, between late December and early January, you will receive a very important IRS letter, assigning you an Identity Protection Personal Identification Number (IP PIN). Please send us a copy of this letter and keep a copy for yourself. This IP PIN may or may not be issued for your 2021 filing depending on whether the IRS has processed 2020 return yet, but it will be an additional layer of protection to you.

What You Can Do:

- **Please provide us with the balance of your tax information needed to prepare your 2020 tax return. Your return must be paper filed, rather than e-filed.**
- Given the breadth of information exposed, we strongly recommend you are **vigilant in reviewing all bank account and brokerage statements, as well as free credit reports.**
- We suggest that you **change the bank account numbers you provided us**, and/**or have a conversation with your bank** regarding the monitoring to be provided by them as well as yourselves. It is also recommended that you change your **passwords** on all accounts, bank and brokerage.
- **We also suggest you contact** the Federal Trade Commission **(FTC)**: 1-877-438-4338 and the Social Security Administration **(SSA)**: 1-800-772-1213 to file a fraud alert.
- **If you have not already done so, please place a 90-day fraud alert on your accounts.** If you want to pursue that further, their contact information is:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	https://www.experian.com/fraud/center.html	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

- You are also entitled to a free credit report every year from each of these three agencies at: www.annualcreditreport.com
- **If you suspect (additional) identity theft, report it to law enforcement including the FTC at https://www.identitytheft.gov/Assistant#**

Our apologies for this lengthy letter, but we want to proactively assist you with the best advice regarding ID Theft. We look forward to working together to resolve the issues with the tax agencies on your behalf.

Sincerely,

Cozby & Company LLC